(12) UK Patent Application (19) GB (11) 2 380 913 (13) A

(43) Date of A Publication 16.04.2003

(21) Application No 0124635.4

(22) Date of Filing 13.10.2001

(51) INT CL[7]
H04L 9/32 9/30

(52) UK CL (Edition V)
H4P PDCSA PDCSC

(56) Documents Cited
GB 2336512 A
EP 1091285 A
EP 0935182 A1
WO 2000/005642 A1

(58) Field of Search
Other: ONLINE : EPODOC, WPI, JAPIO

(71) Applicant(s)
Hewlett-Packard Company
(Incorporated in USA - Delaware)
3000 Hanover Street, Palo Alto,
California 94304, United States of America

(72) Inventor(s)
Cheh Goh
David A Clarke

(74) Agent and/or Address for Service
Richard Anthony Lawrence
Hewlett-Packard Limited, IP Section,
Filton Road, Stoke Gifford, BRISTOL,
BS34 8QZ, United Kingdom

(54) Abstract Title
Remote printing

(57) A method of printing a document (10) stored at a home computing system (5) on a printer (9) of a remote computing system, the home and remote computing system including a home trusted print proxy (HTPP) (3) and a remote trusted print proxy (RTPP) (2), respectively, which are configured to be able to establish communication via a communications link, in which the printer (9) includes a digital identification device (1) configured to provide a printer public key of a cryptographic public key/private key pair and the RTPP (2) is configured to supply a one time token on request, the method including the steps of using a mobile device (4) to interrogate the RTPP (2) and printer (9) to obtain a one time token and the printer public key using the mobile device (4) to transmit to the home computing system (5) a print request including the one time token and printer public and identification of the document (10) to be printed establishing a secure communications channel between the home and remote computing system via at least the HTPP and RTPP the home computing system (5) transmitting the document encrypted by the printer public key to the printer (9) via the secure communications channel and the printer (9) decrypting the encrypted document and initiating printing of the document only if the mobile device is in communication with the printer (9).

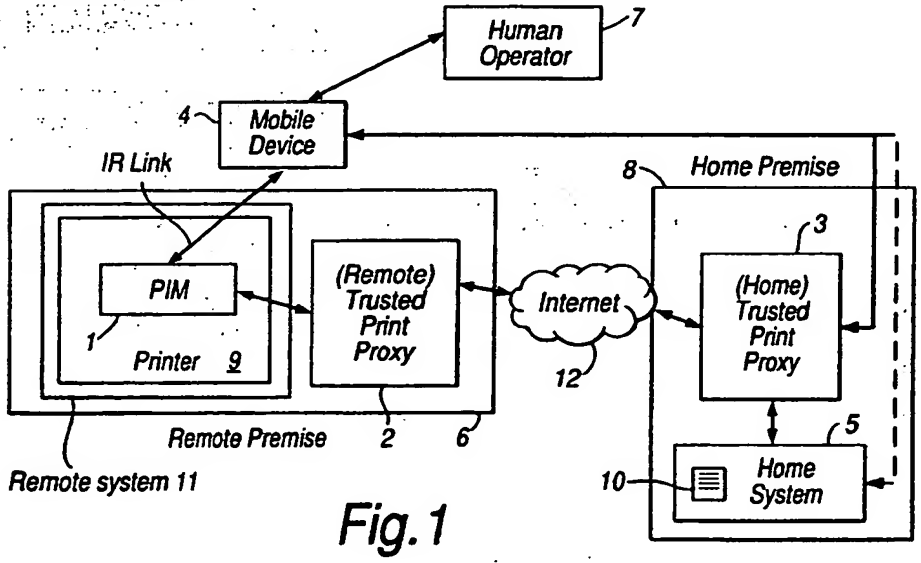

Fig. 1

GB 2 380 913 A

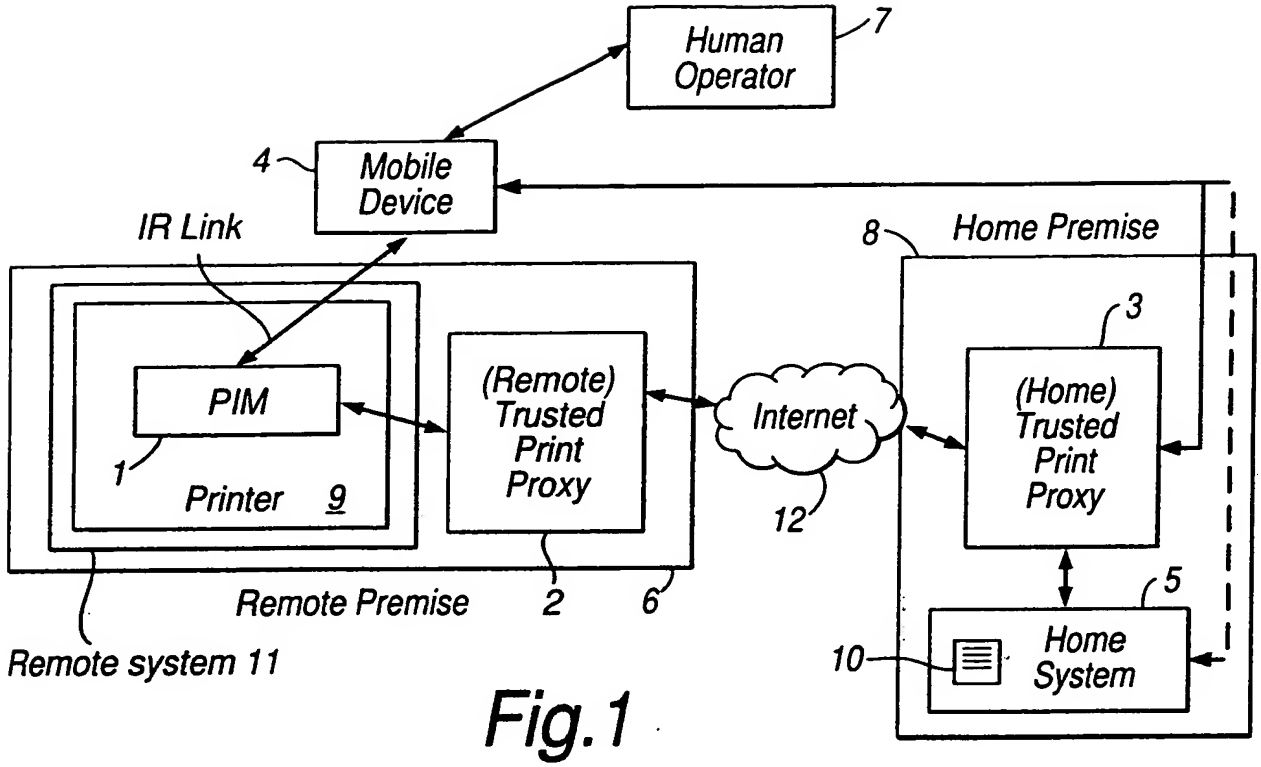
Human Operator
7
4
Mobile Device
IR Link
8
Home Premise
3
PIM
1
Printer 9
(Remote) Trusted Print Proxy
Internet
12
(Home) Trusted Print Proxy
5
Home System
10
Remote Premise
2
6
Remote system 11

Fig.1

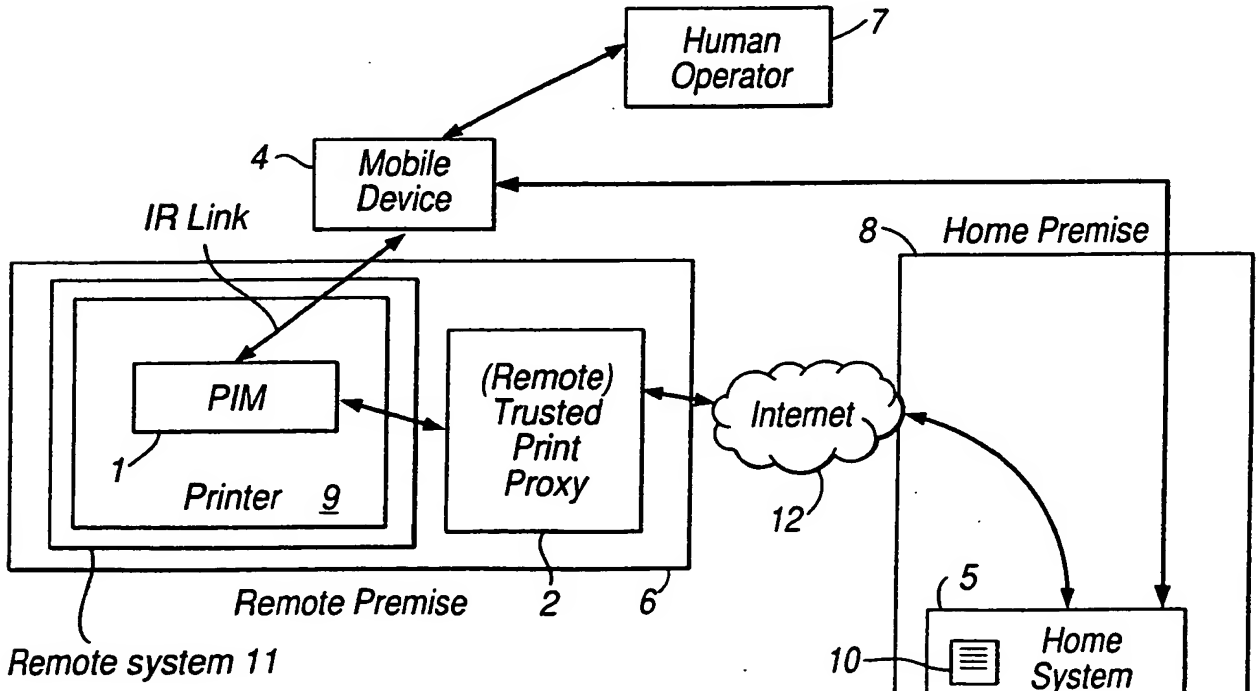
Human Operator
7
4
Mobile Device
IR Link
8
Home Premise
PIM
1
Printer 9
(Remote) Trusted Print Proxy
Internet
12
5
Home System
10
Remote Premise
2
6
Remote system 11

Fig. 4

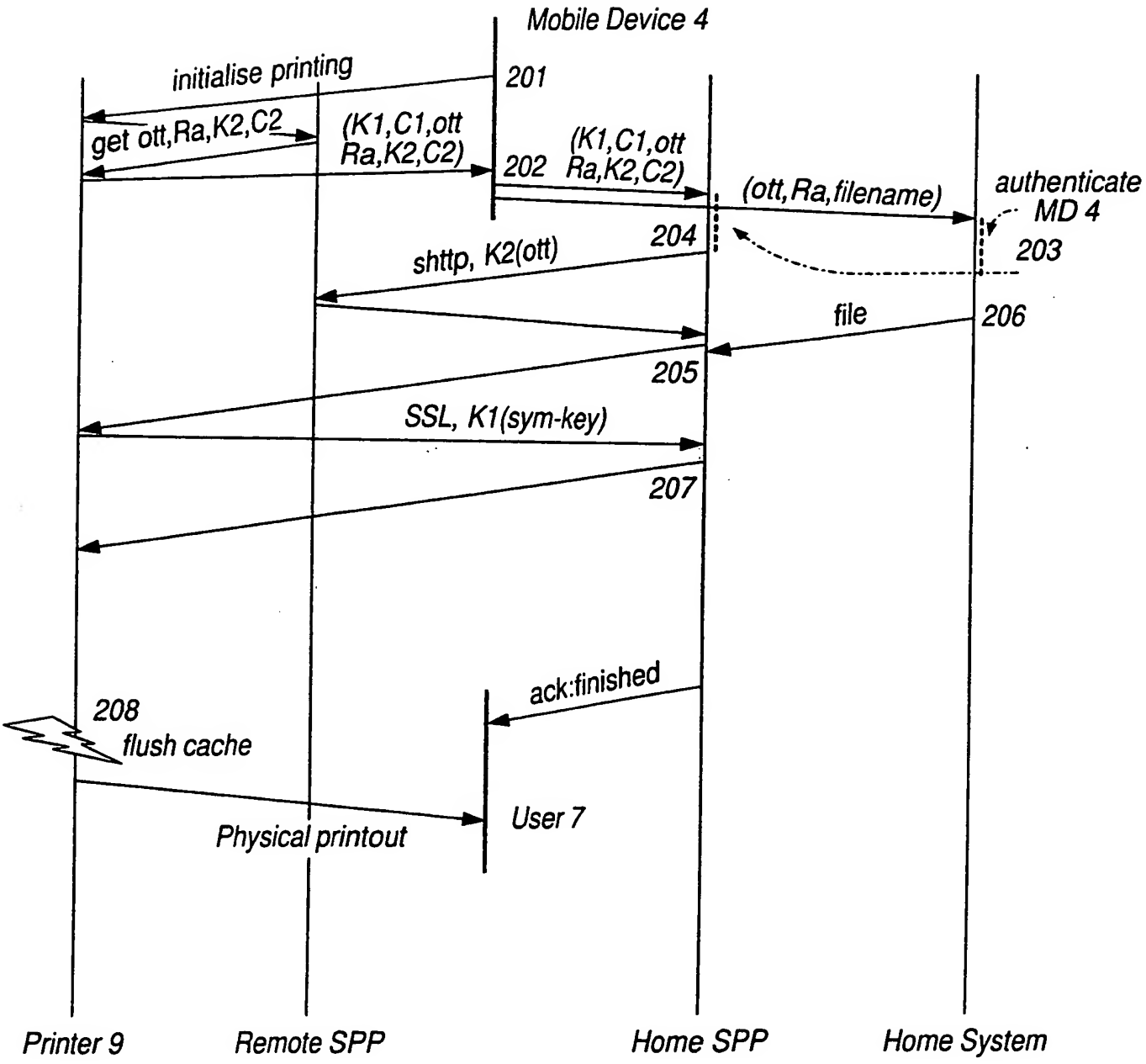
Mobile Device 4
initialise printing
201
get ott,Ra,K2,C2
(K1,C1,ott Ra,K2,C2)
202
(K1,C1,ott Ra,K2,C2)
(ott,Ra,filename)
authenticate MD 4
203
204
shttp, K2(ott)
file
206
205
SSL, K1(sym-key)
207
ack:finished
208
flush cache
User 7
Physical printout
Printer 9
Remote SPP
Home SPP
Home System

Fig.2

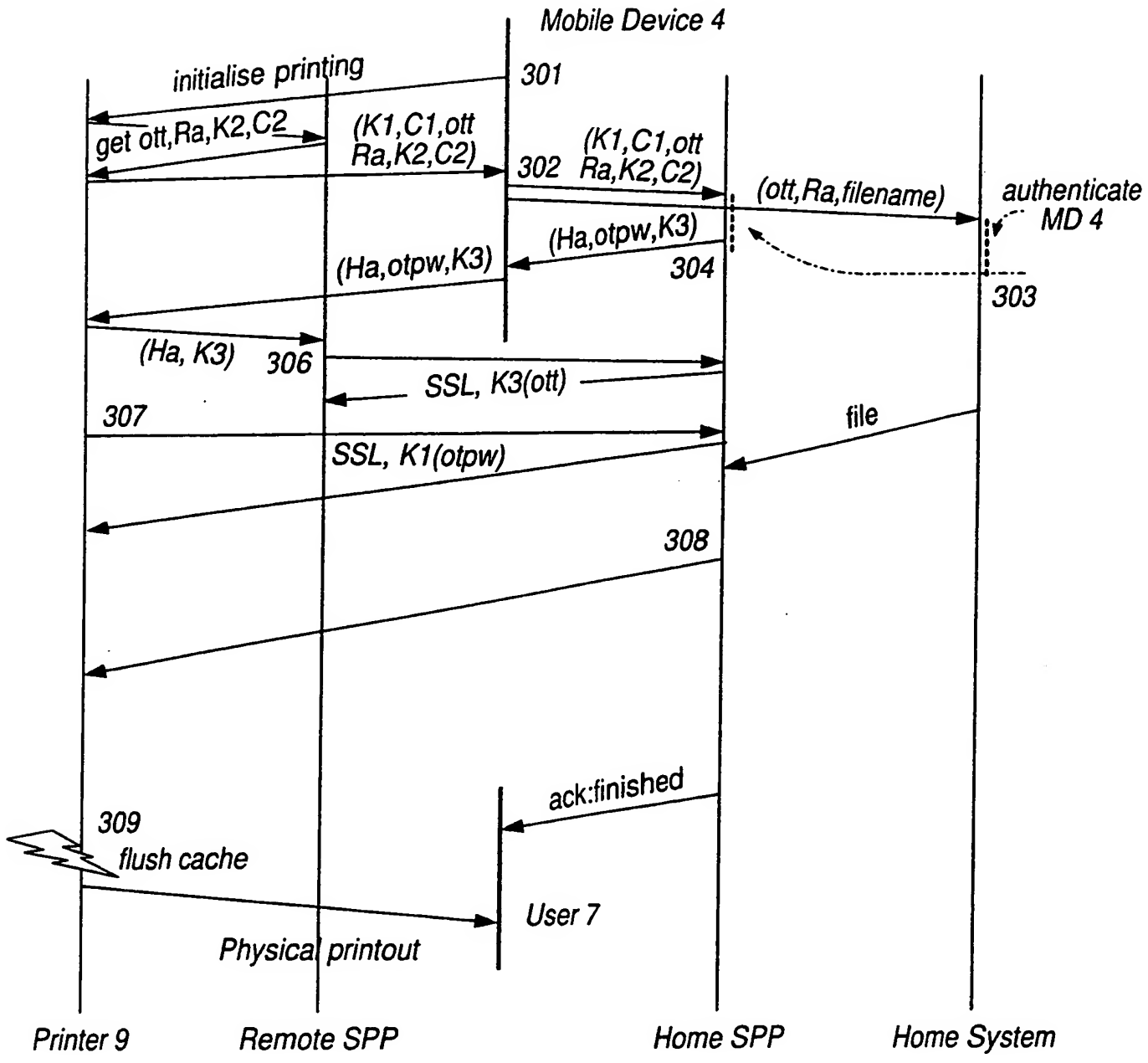
Mobile Device 4
initialise printing
301
get ott,Ra,K2,C2
(K1,C1,ott Ra,K2,C2)
302
(K1,C1,ott Ra,K2,C2)
(ott,Ra,filename)
authenticate MD 4
(Ha,otpw,K3)
304
(Ha,otpw,K3)
303
(Ha, K3)
306
SSL, K3(ott)
307
file
SSL, K1(otpw)
308
ack:finished
309
flush cache
User 7
Physical printout
Printer 9
Remote SPP
Home SPP
Home System

Fig.3

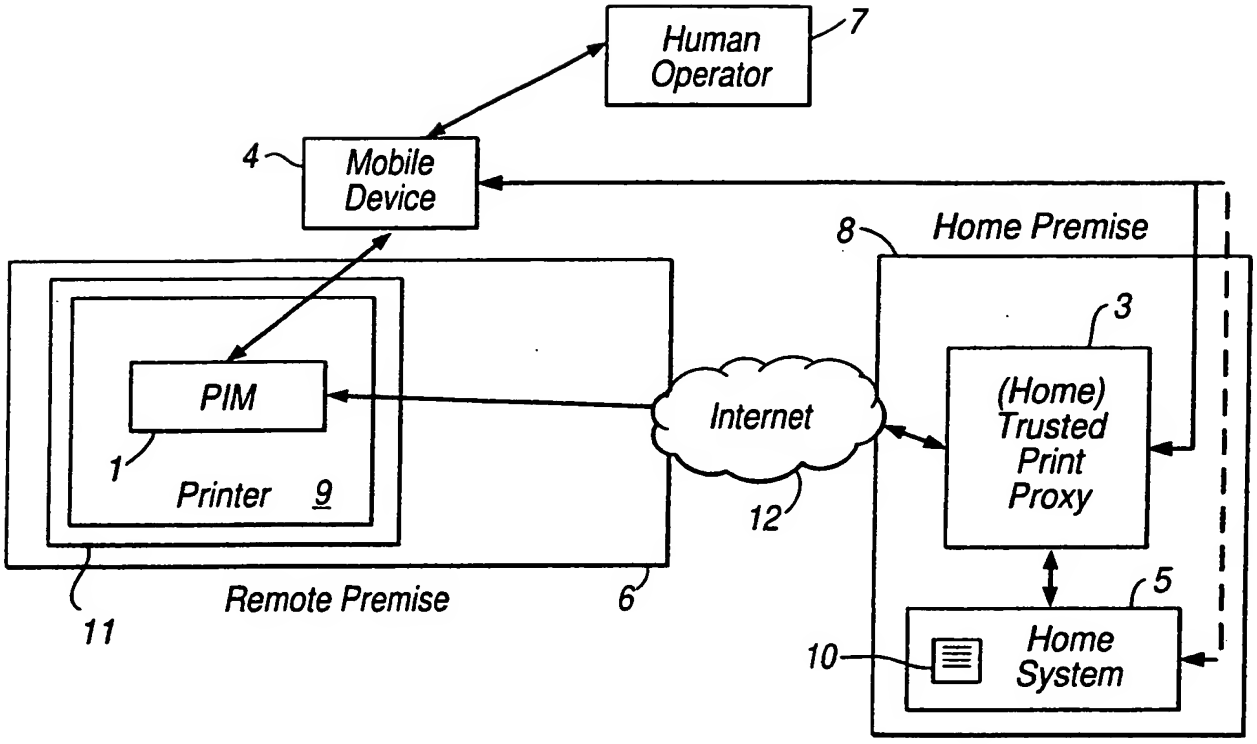
Human Operator
7
4
Mobile Device
8
Home Premise
3
PIM
1
Printer 9
Internet
(Home) Trusted Print Proxy
12
5
Home System
10
Remote Premise
6
11

Fig.5

REMOTE PRINTING

BACKGROUND OF THE INVENTION

There is often a need to print documents away from a user's home environment. For example, travelling sales persons at customer sites, or visitors to competitor/collaborator's locations, often need to print documents not only from the portable device they carry, but also from the file system in their home location. Printing in an environment that is considered as potentially *hostile* requires not only a guarantee that there is protection of the information sent from the home environment to within the foreign environment and in transit through the internet, but also that the security of the hosting foreign environment is not compromised.

For example, consider a person from company X who has important confidential documents stored in his home storage system. He is visiting a competing company, Y, with a view to establish a collaboration project. This is a preliminary investigation and consequently there is very little safeguard with respect to disclosure of information apart from a standard non-disclosure agreement from the legal department.

This person travels with his mobile device, such as a WAP phone, but nothing else as he does not expect too much progress to be made. Half way through the meeting with company Y, the person decides that he needs to retrieve some confidential information from his home system in order to be able to continue with the discussion.

It may well be that company X does not allow any confidential files to be transported out of the home system and has a configuration to disallow ports that might be used for printing. In the same way, company Y may not allow any

and the printer decrypts the encrypted document and initiates printing of the document.

After establishing a secure communication channel between the first and second computing system via the HTPP and RTPP the first computing system transmits the document encrypted by the printer public key to the printer via the secure communication channel and the printer decrypts the encrypted document and initiates printing of the document. The printer may be configured to initialise printing only if the mobile device is in communication with the printer, for example, line-of-sight communication. The printer may be configured to cease printing if the communication link to the mobile device is interrupted for a predetermined, continuous period of time, for example, for 5 or 10 seconds.

Suitable mobile device-printer communications links also include wireless protocols such as "Bluetooth" technology and IEEE 802.11 wireless LAN standard technology or by wire such as serial or parallel port connections or universal serial bus (USB) connections.

The method may use PKCS7 to establish symmetric-key keying material for efficient encrypted communications.

Embodiments of the invention can provide the following advantages to the person at a remote computing system:

uniqueness: the ability to go to a printer and get a printout, knowing that no other printer is able to render a hard copy using the information in that transaction;

confidentiality: nobody, apart from that specific printer, outside the traveller's home environment has access to the content printed in that printer, as a result of carrying out that transaction. The information is permanently destroyed immediately after rendering the printing;

invention also provides a computing system adapted to allow secure printing by a user at a remote location, wherein the computing system and a user account are within a common firewall; wherein said computing system is programmed to provide a home trusted print proxy (HTPP), wherein on request the HTPP is adapted to send a one-time password, the network address of the HTPP and the HTPP public key of cryptographic public/private key pair to a mobile device of the user, and wherein on verification of the one-time password received from a remote printer, the HTPP establishes a secure communications channel with the remote printer and transmits documents encrypted by a public key of the printer to the printer.

Other aspects of the invention will become apparent from the following description of an exemplary embodiment taken in conjunction with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a schematic diagram of a first system for implementing methods according to the present invention;

Figure 2 is a schematic flow diagram of a first embodiment of the method of the present invention;

Figure 3 is a schematic flow diagram of a second embodiment of the method of the present invention;

Figure 4 is a schematic diagram of a second system for implementing methods according to the present invention; and

Figure 5 is a schematic diagram of a third system for implementing methods according to the present invention.

There are at least two ways to enable secure remote printing with such a system. They are the Push model and the Pull model.

Referring now to Figure 2, there is illustrated a method of the present invention in which the printing is effected by the PUSH model including the following steps 201 to 208.

201. User 7 uses mobile device 4 to get K1 the public key and C1 the optional certificate of the printer 9 from its PIM 1, a one time token (ott) from the Remote Trusted Print Proxy (RTPP) 2, Ra the network address of the RTPP 2 and K2 the public key and C2 the optional certificate of RTPP 2 via the printer 9, using, for example, the IR port. The certificates C1 and C2, if employed could include the respective public keys K1 and K2.

202. User 7 will, securely through mobile device 4, use some form of authentication methods to identify herself to the Home Trusted Print Proxy (HTPP) 3, and Home System (HS) 5. She then proceeds to send, in this example, a print request containing K1, C1, ott, Ra, K2, C2 and filename, where filename is the name of the document 10 to be printed in the printer 9.

203. The HTPP 3 and HS 5 verify that the request has been sent by the user and its mobile device.

204. If the public keys K1 and K2 are encapsulated in respective digital certificates C1 and C2, then an additional step of checking the certificates C1 and C2 can be carried out by the home system 5 to establish that they come from a printer and a TPP made by manufacturers who guarantee the machine's behaviour for enabling Trusted Remote Printing.

205. The HTPP 3 will use Ra to contact RTPP 2, and use K2 to establish a secure communication link with RTPP 2, using ott to authenticate itself as the intended source of print contents, for that session.

302. User will, securely though mobile device 4, use some form of authentication methods to identify herself to the Home Trusted Print Proxy (HTPP) 3, and the home system (HS) 5. She then proceeds to send a print request containing K1, C1, ott, Ra, K2, C2 and filename, where filename is the name of the document to be printed in the printer 9.

303. The HTPP 3 and HS 5 verify that the request has been sent by the user and its mobile device.

304. After verification, the HTPP 3 will send a one-time password otpw, its network address Ha and its public key K3 to the mobile device 4.

305. User 7 uses mobile device 4 to send printer 9 the otpw, the address Ha and K3 from HTPP, and asks printer 9 to accept a print job from HS 5. Printer 9 asks the RTPP 2 to connect to HTPP 3 using Ha and K3. The otpw never leaves the printer 9 unencrypted.

306. RTPP 2 contacts HTPP 3 using K3 and authenticates itself with HTPP 3 using ott in order to establish a secure channel.

307. The printer 9 authenticates itself as the target printer by encrypting the otpw with K3 and sends it to the HTPP 3.

308. The HTPP 3, upon verifying the otpw, will establish an encrypted channel to send the print image to the printer 9. The RTPP will be acting as a bridge between the printer and the HS 5. The user 7 must, in this embodiment, maintain physical vicinity with the printer 9 using the IR connection of the mobile device in order for the printer 9 to continue printing. The printer 9 will send the ID of the mobile device back to the HTPP 3 as indication that the mobile device owner continues to receive the physical printed output. If the IR contact is disrupted for more than certain amount of time, for example, 10 seconds, the

port 80, the http port, it is reasonable to add the IP address of the TPP to the firewall configuration. In this way, the TPP will be able to accept outside connections, and carry out its function as depicted in the above embodiments. A home TPP is used in the "push" model, while a remote TPP is used in the "pull" systems of Figures 3 and 4. As mentioned, they are not strictly necessary. However, in terms of practical implementation, it is desirable to use them. There are several reasons for doing so.

Having an HTPP on site means that potentially all members of the entity will be able to print while on the move, using the "pull" method described above if they come across a printer with a PIM. Secondly, a TPP can become the control point that checks legitimacy of printing documents outside the home site. It is easier to manage out of site printing from a single location, according to the current policy, than to manage it from every possible home system which might send documents to a remote printer. Furthermore, an HTPP can act as the remote print spooler, having a number of print drivers to render documents according to the remote printer type. It is not desirable that every home system has a similar repertory of print driver and the formatting of document using one of the drivers.

A TPP effectively serves as an RTPP if the site is now visited by a travelling user from outside. If the site is somewhere like a conference venue, hotel business centre, or business lounge, then being equipped with an RTPP will enable the site to provide TRPS to its visitors using the "pull" model, regardless of whether the visitors have a TPP at their home site. Even if the remote site is not providing facilities to its visitor as a business, so long as it has two or more printers made available for use by visitors, the configuration of the firewall will have to cater for each printer so that http traffic from the outside firewall through port 80 can go through. It is not good practice to have to configure the firewall with the IP addresses of all the printers. Putting a TPP on the inside so that only one IP address with the http port open is preferable. In addition to this simplification of the firewall administrator's task, the TPP can prevent security

visited. If a patient has an insurance policy and the location of his or her medical history is known, there will still be great difficulty in retrieving that information in the emergency room.

Suppose the ER have a PIM enabled printer which has a further additional digital certificate that certifies that it is used by the emergency services, then the systems that keep the medical record can potentially use the public key of the printer and the TPP to render information at the point where the patient needs to be treated. In fact, the point of rendering can even be by an ambulance, or a mountain rescue station and so forth.

Clearly, additional safeguard is needed regarding how the smart card of the duty medical personnel and of the patient, if any, may be needed in conjunction with a modified protocol to achieve medical history rendering. This will depend on the requirements and must undergo a different analysis to arrive at the appropriate process.

The foregoing description has been limited to a specific embodiment of this invention. It will be apparent, however, that variations and modifications may be made to the invention, with the attainment of some or all of the advantages of the invention. Therefore, it is the object of the appended claims to cover all such variations and modifications as come within the true spirit and scope of the present invention.

4. A method as claimed in claim 3, in which the mobile telephone is configured to perform the interrogation by any one of an infra-red communications link, a wireless protocol or by a wire connection between the mobile device and the printer.

5. A method as claimed in claim 1, in which the digital identification device is also configured to provide a printer digital certificate.

6. A method as claimed in claim 1, in which the printer public key is in the form of a printer digital certificate.

7. A method as claimed in claim 6, in which the printer digital certificate is presented for acceptability.

8. A method as claimed in claim 1, in which the mobile device provides authentication data to the home computing system prior to transmitting the print request.

9. A method as claimed in claim 1, in which the printer is configured to stop printing and the printer memory is flushed if the mobile device breaks communication with the printer for a predetermined, continuous period of time.

10. A method as claimed in claim 1 in which the printer memory is flushed after printing.

11. A method as claimed in claim 1, in which the printer is configured to initialise printing of the document only if the mobile device is in communication with the printer.

12. A method as claimed in claim 11, in which the printer is further configured to stop printing and the printer memory is flushed if communication between the

the printer issues a request to the HTPP using the HTPP network address and HTPP public key using the one-time password as authentication and establishes the secure communications channel with the HTPP,

the printer authenticates itself to the HTPP by encrypting the one-time password using the HTPP public key,

the HTPP upon verifying the one-time password establishes the secure communications channel with the printer whereupon the first computing system transmits the documents encrypted by the printer public key to printer via the secure communications channel.

15. A method of claim 2, in which the home computing system includes a home trusted print proxy (HTPP), and the remote computing system includes a remote trusted print proxy (RTPP), the RTPP including a digital identification device configured to provide an RTPP public key of a cryptographic public key/private key pair and is configured to supply a one-time token on request; and in which the HTPP sends a one-time password, the network address of the HTPP and the HTPP public key of cryptographic public/private key pair to the mobile device,

the user sends the network address of the HTPP and the home system public key of cryptographic public/private key pair to the printer with a request that the printer accept printer instructions from the HTPP,

the printer issues a request to the RTPP to connect to the HTPP using the HTPP network address and HTPP public key,

the RTPP contacts the HTPP using the HTPP public key using the one time token as authentication and establishes the secure communications channel with the HTPP,

the printer authenticates itself to the HTPP by encrypting the one-time password using the HTPP public key,

the HTPP upon verifying the onetime password establishes the secure communications channel with the printer whereupon the first computing system

the HTPP upon verifying the one-time password and using the public key of the printer to authenticate the printer establishes the secure communications channel with the printer, whereupon the home system transmits the document encrypted by the printer public key to the printer via the secure channel.

17. The method of claim 1, in which the encryption key is the printer public key.

18. The method of claim 1, in which the printer public key is presented in the form of a digital certificate signed by the printer manufacturer.

19. The method of claim 1, in which the encryption key is a symmetric session encryption key, the method including using the public key as an enveloping key for sending the symmetric session key to the token issuer securely.

20. A computing system adapted to allow secure printing by a user at a remote location, wherein the computing system and a printer for said secure printing are within a common firewall; wherein said computing system is programmed to provide a remote trusted print proxy (RTPP), and the RTPP includes a digital identification device configured to provide an RTPP public key of a cryptographic public key/private key pair and is configured to supply a one-time token on request, wherein on request by the printer the RTPP provides the RTPP public key, the RTPP network address and the RTPP one-time token, and wherein on contact by a user's home computing system the RTPP is configured to accept the one-time token as authentication and to establish a secure channel with the user's home computing system.

21. A computing system adapted to allow secure printing by a user at a remote location, wherein the computing system and a user account are within a common firewall; wherein said computing system is programmed to provide a home trusted print proxy (HTPP), wherein on request the HTPP is adapted to

21

The Patent Office

INVESTOR IN PEOPLE

Application No: GB 0124635.4 **Examiner:** Ken Long
Claims searched: 1 to 21 **Date of search:** 12 June 2002

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.T): None

Int Cl (Ed.7): None

Other: ONLINE : EPODOC, WPI, JAPIO

Documents considered to be relevant:

Category	Identity of document and relevant passage		Relevant to claims
X	GB 2336512 A	INTEL (page 3 lines 18 to 30, page 5 line 30 to page 6 line 20, page 7 lines 23-26 and page 8 lines 16-27)	1, 20 and 21 at least
A	WO 00/05642 A1	TUMBLEWEED (page 5 line 24 to page 6 line 7)	20
A	EP 1091285 A2	CANON (column 2 lines 11-28	None
A	EP 0935182 A1	HEWLETT-PACKARD (column 8 lines 42-48 and column 9 line 43 to column 10 line 6)	None

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.